**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re the application of :

| | | | |
|---|---|---|---|
| Appl. No. | : | 09/435,899 | Confirmation No. 5856 |
| Applicant | : | P. J. Seger | |
| Filed | : | 11/08/1999 | |
| TC/A.U. | : | 2175 | |
| Examiner | : | J. F. Betit | |
| Docket No. | : | TU999050US1 | |

Title: WIRELESS SECURITY ACCESS MANAGEMENT FOR A PORTABLE DATA STORAGE CARTRIDGE

**THIRD DECLARATION UNDER 37 C.F.R. Section 1.132**

I, Paul M. Greco, declare and say:

That I am a citizen of the United States of America and I reside at 2791 W. Woodview Crest Drive, Tucson, AZ 85742, USA.

That I am a Senior Programmer at IBM Systems Group, in the field of tape drive microcode development, since April 1996.

That I was previously a Senior Design Engineer at Environmental Systems Products, Inc., in the field of code and systems architecture and development, from August 1990 to April 1996.

That I attended college from 1987 to 1988 at the University of Arizona, located in Tucson, AZ.

That I am knowledgeable in the technology and science of Computer Science and Computer Engineering.

**1) Present U. S. Patent Application Serial No. 09/435,899**

That I have reviewed the present U. S. Patent Application Serial No. 09/435,899, and find that it describes "a portable security system *** which resides in a portable data storage

cartridge for managing access to the portable data storage cartridge". (Page 3, lines 13-16).

**a)** Security of access is conducted by combining a user authentication message from the user with the unique user identifier in the user table. "A programmable computer processor is mounted in the portable data storage cartridge and coupled to the wireless interface. *** The computer processor provides a user table comprising at least one unique user identifier for each authorized user, *** and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user." (Page 4, lines 2-14) (emphasis added).

"The computer processor *** receives user authentication messages from the data storage drive via the wireless interface and combines the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity". (Page 4, lines 15-21) (emphasis added).

"Preferably, a private key, public key cryptographic algorithm is employed. Thus, each user identifier in the user table comprises a user symbol and the user's decrypting sender public key, wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, specifically comprising a request for access encrypted by a sender private key and a receiver public key, and wherein the employed private key, public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, whereby the user authentication message is known to have come from the user." (Page 4, line 22 - Page 5, line 9) (emphasis added).

**b)** Certain users are permitted management of access, and that access is portable. "The permitted activities in the user table may comprise *** 5) add entries to the user table, and 6) change/delete entries to the user table." (Page 5, lines 10-16) (emphasis added).

**2) International Publication No. WO 87/07062, Anderl et al.**

That I have reviewed International Publication No. WO 87/07062, Anderl et al., and find that it relates to a "high security portable data carrier system ***" (Page 2, lines 7-8), with "an executive operating system that is accessed from the station via a set of *** command primitives" which "manipulate the card file system in accord with rules required by card security" (Page 2, lines 17-20).

**I-III)** The discussion of Anderl et al. of my Second Declaration Under 37 C.F.R. Section 1.132 is incorporated herein.

**a)** "Security for the card is provided by requiring a separate password for gaining access to each of designated levels of interaction between the card and the associated station." (Anderl et al. Page 2, lines 27-29) (emphasis added). "This password is checked internally by the card algorithmically against the appropriate password at the same login level in the card header." (Page 11, lines 16-18) (emphasis added). Any authentication (not directly described) appears to be of the "card" or "file" and not the "user", see Page 7, lines 9-19.

Thus, Anderl et al. access security is provided by an entirely different mechanism than the present '899 Application's "unique user identifier for each authorized user, ***. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user."

Further, Anderl et al. fail to encrypt the access process. "In addition, encryption of data as it is provided to the card is also available for those particular sensitive applications." (Page 3, lines 21-23) (emphasis added). Without encryption of the access process, communication across an Anderl et al. interface, including the password itself, is in the open.

Thus, Anderl et al. is further distinguished from the present '899 Application, "wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, *** whereby the user authentication message is known to have come from the user." (Page 4, line 22 - Page 5, line 9) (emphasis added).

**b)** Anderl et al. do not provide management of access as part of the operational process, nor portability of that management.

Rather, Anderl et al. discuss establishment of access at issuance by the issuer at a particular station. "The high security header 35 contains information such as *** the passwords for each login level ***. Direct access to the header section is available only to the two top security levels." (Page 9, lines 4-9). "The fourth level of security is that retained by the MASTER ISSUER. It is at this level that the card is formatted and from which it is issued. *** Each account in this example is handled by a separate file on the card and only persons or programs with the proper credentials for a particular file may access that file at an appropriate application station." (Page 8, lines 6-15). This level is assumed despite the naming of "DEVELOPER and SUPER USER" as the top two security levels, see Page 8, lines 16-25. Thereafter, a pasword "can be rewritten by logging into the card at a higher security level ***" (Page 3, lines 9-11), but there is no access management.

Thus, Anderl et al. access is established at issuance of the card, and is limited to a particular station, making it non-portable, as opposed to the present '899 Application in which certain users are permitted management of access, and that access is portable. "The permitted activities in the user table may comprise *** 5) add entries to the user table, and 6) change/delete entries to the user table." (Page 5, lines 10-16) (emphasis added).

**3) U. S. Patent No. 4,956,769, Smith**

That I have reviewed U. S. Patent No. 4,956,769, Smith, and find that it relates to a security system for a fixed installation, "in a computer system" (Column 1, line 58), and "capable of limiting the access of some selected users and terminal locations to *** operations on selected database records and fields." (Column 1, lines 9-12).

**a)** Smith fails to provide user authentication, relying instead on the normal fixed installation logon process "at least one system user, identified by a 'userid' or unique user identification symbol, that is accessing the system from at least one terminal location with a terminal address," (Column 1, lines 58-62). "Specifically, the user access profile table and the terminal location security access table are constructed within the host system environment ***." (Column 5, lines 9-13).

Thus, Smith has no relationship to the present '899 Application's "unique user identifier for each authorized user, ***. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user."

Further, Smith fails to provide encryption, thus further distinguising Smith from the present '899 Application, "wherein

the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, *** whereby the user authentication message is known to have come from the user." (Page 4, line 22 - Page 5, line 9) (emphasis added).

**b)** Smith does not provide management of access as part of an operational process, nor portability of that management.

Rather, Smith discusses "membership of any one given user can be changed by the security systems programmer at the installation time" for the host system. (Column 4, lines 10-14). "Specifically,the user access profile table and the terminal location security access table are constructed within the host system environment ***. After this, each of the respective tables is built ***" (Column 5, lines 9-21).

Thus, Smith access is established at installation time, and is conducted within the host system, making it non-portable, as opposed to the present '899 Application in which certain users are permitted management of access, and that access is portable. "The permitted activities in the user table may comprise *** 5) add entries to the user table, and 6) change/delete entries to the user table." (Page 5, lines 10-16) (emphasis added).

That the undersigned declares further that all statements made herein of his own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

Further declarant saith not.

Date: ~~DEC~~ 2, 2004 /s/ Paul M. Greco

Paul M. Greco